(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: 0 477 039 A2

(12) EUROPEAN PATENT APPLICATION

(21) Application number: 91308667.4

(51) Int. Cl.[5]: G06F 9/445

(22) Date of filing: 20.09.91

(30) Priority: 21.09.90 JP 252864/90

(43) Date of publication of application:
25.03.92 Bulletin 92/13

(84) Designated Contracting States:
DE FR GB

(71) Applicant: KABUSHIKI KAISHA TOSHIBA
72, Horikawa-Cho Saiwai-ku
Kawasaki-shi Kanagawa-ken (JP)

(72) Inventor: Nukui, Harumi, c/o Intellectual Property Division
Kabushiki Kaisha Toshiba, 1-1, Shibaura 1-chome
Minato-ku, Tokyo (JP)

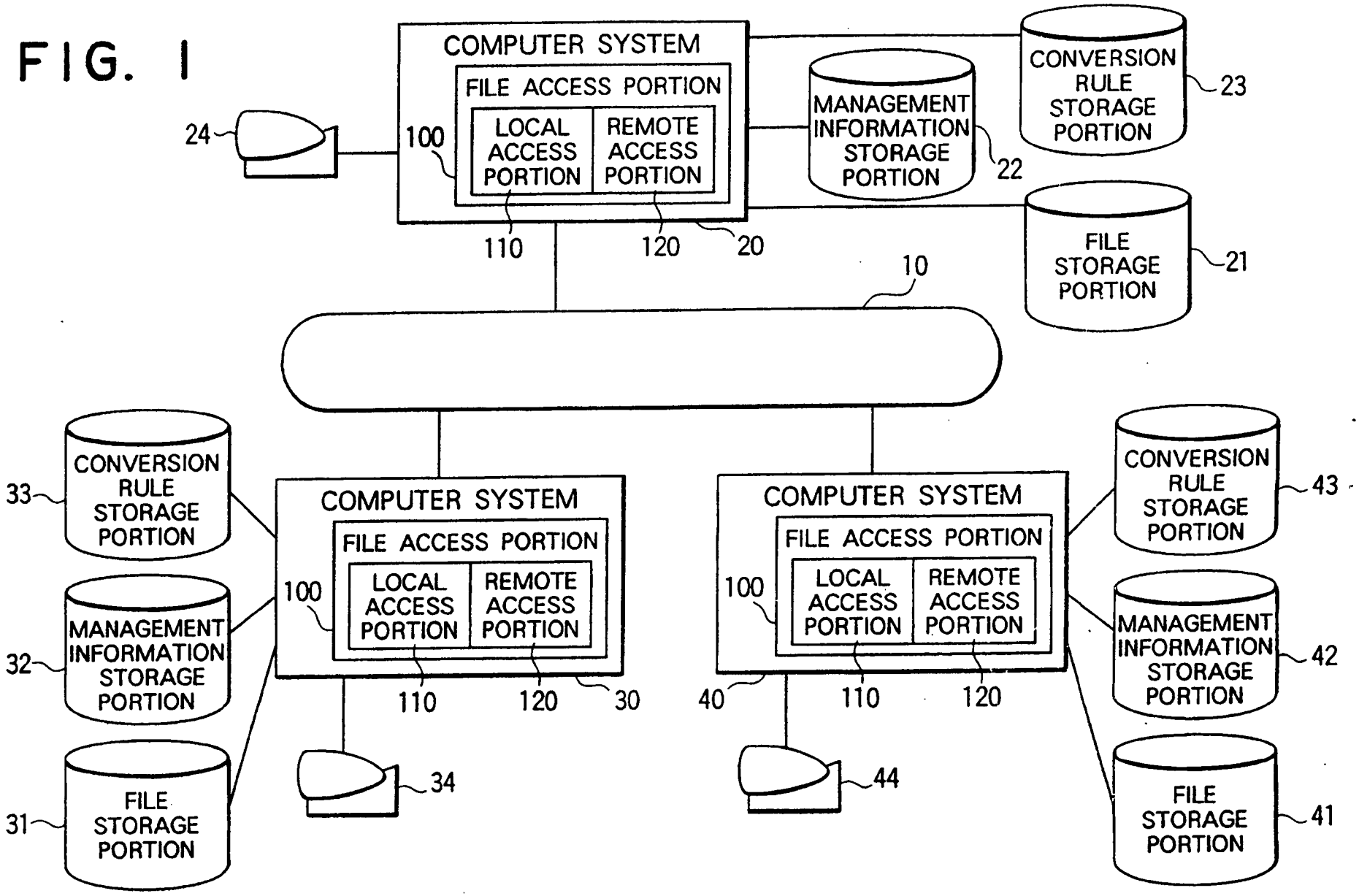
(74) Representative: Luckhurst, Anthony Henry William et al
MARKS & CLERK 57-60 Lincoln's Inn Fields
London WC2A 3LS (GB)

(54) Computer network.

(57) Each computer system of the computer network according to the present invention has a management information storage portion for storing information with respect to an access authority in accordance with an owner ID and a conversion rule storage portion for storing a rule for converting the formats of a user ID and an access authority. Each computer system adds a machine ID to a user ID and sends the resultant ID to another computer system when a remote access request is issued. In addition, the computer system determines whether or not the formats of the user ID and the access authority being received accord with those of a local computer system when a remote access is accepted. The computer system converts the formats of the user ID and the access authority being received into those of the local computer system in accordance with a predetermined conversion rule when the formats of the local computer system are not matched with those on the remote computer system. Thereafter, the computer system compares the user ID and the access authority whose formats have been converted with information of the access authority stored in the access authority storage portion and determines whether or not to execute the remote access.

EP 0 477 039 A2

FIG. 1


COMPUTER SYSTEM
FILE ACCESS PORTION
LOCAL ACCESS PORTION
REMOTE ACCESS PORTION
100
110
120
20
24
MANAGEMENT INFORMATION STORAGE PORTION
22
CONVERSION RULE STORAGE PORTION
23
FILE STORAGE PORTION
21
10
CONVERSION RULE STORAGE PORTION
33
MANAGEMENT INFORMATION STORAGE PORTION
32
FILE STORAGE PORTION
31
COMPUTER SYSTEM
FILE ACCESS PORTION
LOCAL ACCESS PORTION
REMOTE ACCESS PORTION
100
110
120
30
34
COMPUTER SYSTEM
FILE ACCESS PORTION
LOCAL ACCESS PORTION
REMOTE ACCESS PORTION
100
40
110
120
44
CONVERSION RULE STORAGE PORTION
43
MANAGEMENT INFORMATION STORAGE PORTION
42
FILE STORAGE PORTION
41

The present invention relates to a computer network for connecting a plurality of computer systems through a communication medium and a method of accessing files thereof.

Thus far, there has been a computer network where the user of a computer system can remotely access a file that another computer system has without necessity of a complicated log-on procedure.

The file access in such a computer network is performed under condition that a user ID and an access authority on the request side are matched with those on the accept side.

However, when the computer type on the request side differs from that on the accept side, because of differences of the formats of the user ID and the access authority, the computer system on the access accept side may not correctly determine the validity of an access request from the computer system on the access request side. In this case, the computer system on the request side has to perform a particular procedure so as to validly access a file that the computer system on the accept side has. Thus, the advantage of the remote access is lost.

Therefore, an object of the present invention is to provide a computer network for validly performing a remote access of files even if the formats of the user ID and the access authority on the access request side differ from those on the access accept side.

To accomplish such an object, the computer network according to the present invention comprises a computer network connected with a plurality of computer systems through a communication medium for accessing files that the plurality of computer systems have from all of the plurality of computer systems, each of the plurality of computer systems comprising access authority information storage means for storing information with respect to an access authority in accordance with an owner ID, means for adding a machine ID to a user ID and for sending the resultant ID to another computer system of the plurality of computer systems when a remote access request is issued, means for determining whether or not the formats of the user ID and the access authority being received accord with those of a local computer system of the plurality of computer systems when a remote access is accepted, means for converting the formats of the user ID and the access authority being received into those of the local computer system of the plurality of computer systems in accordance with a predetermined conversion rule when the formats of the local computer system are not matched with those on the remote computer system, and means for comparing the user ID and the access authority whose formats have been converted with information of the access authority stored in the access authority storage means and for determining whether or not to execute the remote access.

Thereby, according to the present invention, even if the formats of the user ID and the access authority on the access request side differ from those on the access accept side, remote files can be validly accessed.

Fig. 1 is a block diagram showing an overall construction of a computer network of an embodiment according to the present invention;

Fig. 2 is a schema showing a tree construction of a file group that a computer system has;

Fig. 3 is a schema describing relations of file groups that two computer systems have;

Fig. 4 is a table outlining information with respect to access authority;

Fig. 5 is a table outlining a conversion rule;

Fig. 6 is a flow chart showing a flow of a process for issuing an access request;

Fig. 7 is a flow chart showing a flow of a process for determining the validity of a file access; and

Fig. 8 is a flow chart showing a flow of a process performed when a remote access request is accepted.

Fig. 1 is a block diagram showing an overall construction of a computer network of an embodiment according to the present invention.

In the figure, reference numeral 10 is a communication medium. Reference numerals 20, 30, and 40 are computer systems which are connected each other through the communication medium 10. The computer system 20, 30, 40 is connected with a file storage portion 21, 31, 41 for storing a plurality of files, a management information storage portion 22, 32, 42 for storing information necessary for managing a file access, a conversion rule storage portion 23, 33, 43 for storing a conversion rule for compensating differences of the formats of a user ID and an access authority in accordance with a computer type, and a keyboard/CRT 24, 34, 44.

The management information storage portion 22, 32, 42 stores a path to each file stored in the file storage portion 21, 31, 41. A file group stored in the file storage portion 21, 31, 41 is identified by a path which is routed from "ROOT" disposed at the top of the tree construction to a directory d. Thus, the path to a file f1 is represented with "/d1/d11/f1/".

In this computer network, files that other computer systems have can be treated as those that a particular computer system has. For example, assume that two computer systems have respective file groups in a tree construction as shown in Fig. 3. In such a construction, the operator of one computer system A declares that the directory d2 is the same as the directory dr1 between the tree construction of the file group which the computer system A has and that which the computer system B has. Thus, the computer system A can treat a sub file group in the directory dr1 or below of a file group that the computer system B has as a file group in the directory d2 or below that the computer system A has.

The management information storage portion 22, 32, 42 stores information with respect to access authority of each file as information for determining the validity of executing a file access.

Fig. 4 is a table outlining information with respect to access authority. In other words, the information with respect to access authority is composed of an owner ID (a personal ID and a group ID) of each file and an access authority type (for example, read, write, delete, move, and execute) permitted to the owner ID.

In addition, the management information storage portion 22, 32, 42 stores a user ID (a personal ID and a group ID) which is used to request a file access.

In such a construction, a problem takes place when the format of the access authority on the access request side differs from that on the access accept side due to difference of computer types and the like therebetween. For example, when the access authority of one computer system and that of another computer system are set with respect to five types "read, write, delete, move, and execute" and three types "read, write, and execution", respectively, since the access authority on one side does not match that on another side, a file access cannot be validly performed.

To prevent that, in the embodiment according to the present invention, the conversion rule storage portion 23, 33, 34 stores a conversion rule. Fig. 5 shows a table outlining a conversion rule with respect to the access authority. In other words, in the conversion rule, the access request types "delete and move" issued from the computer system B to the computer system A are substituted into the access authority type "write" by the computer system A.

In addition, the conversion rule storage portion 23, 33, 43 also stores another conversion rule for compensating a difference between the format of the user ID on one side and that on the other side.

For example, assume that the user ID is represented with 16 bits in the computer system A and with 32 bits in the computer system B. In this case, as the conversion rule that the computer system A has, a data mapping rule with respect to an ID reading memory area for treating 32 bit data as 16 bit data is defined, while as another conversion rule that the computer system B has, another mapping rule for treating 16 bit data as 32 bit data is defined.

A file access portion 100 of the computer system 20, 30, 40 is functionally categorized as a local access portion 110 for executing a file access in a local computer system and a remote access portion 120 for executing a remote file access with another computer system.

Then, with reference to Figs. 6 to 8, a file access operation in the computer network according to the present invention will be described.

As shown in Fig. 6, when the computer system 20 issues a file access request, the file access portion 100 looks into the presence of a desired file in the file storage portion 21 thereof in accordance with information stored in the management information storage portion 22 (in the step 601).

When the file access portion 100 found the desired file in the local computer system 20, it obtains a personal user ID and a group user ID from the management information storage portion 22 as shown in Fig. 7 (In the step 701).

Thereafter, the file access portion 100 looks into an owner ID (a personal ID and a group ID) stored in the management information storage portion 22 (in the step 702).

Thereafter, the file access portion 100 compares the personal ID of the user ID with that of the owner ID (in the step 703). When they are matched, the file access portion 100 references the access authority in accordance with the owner personal ID (in the step 704).

Thereafter, the file access portion 100 looks into the presence of the type of the real access request which ismatched with one of the types of the access authority being referenced (in the step 705). When the file access portion 100 found the type of the access authority which was matched, it accepts the file access (in the step 706).

When the file access portion 100 could find the type of the access authority which was matched or when it found that the personal ID of the user ID did not accord with that of the owner ID, it compares the group ID of the user ID with that of the owner ID (in the step 707).

When the group ID of the user ID is matched with that of the owner ID, the file access portion 100 references the access authority in accordance with the owner group ID (in the step 708).

Thereafter, the file access portion 100 looks into the presence of the type of the real access request which is matched with one of the types of the access authority being referenced (in the step 709). When the file access portion 100 found the type of the access authority which was matched, it accepts the file access (in the step 706).

When the file access portion 100 could not find the type of the access authority which was matched or when it found that the personal ID of the user ID did not accord with that of the owner ID in the step 707, it references another type of the access authority (in the step 710).

Thereafter, the file access portion 100 looks into the presence of the type of the real access request which is matched with one of the types of the access authority being referenced (in the step 711). When the file access portion 100 found the type of the access authority which was matched, it accepts the file access (in the step 706). When the file access portion 100 could not find the type of the access authority

which was matched, it prohibits the file access (in the step 712).

When the file access portion 100 determined that the desired file was present in another computer system 30, 40 in the step 601, it adds a machine ID of the local computer system 20 to the user ID (the personal ID and the group ID) in the management information storage portion 22 (in the step 602) and then sends them to another computer system 30, 40 so as to issue a remote access request (in the step 603). Thereafter, the file access portion 100 enters a standby state for waiting for a response from the other computer system 30, 40.

The file access portion 100 of the other computer system 30, 40 which accepted the remote access request receives the user ID (in the step 801) and looks into the machine ID from the user ID being received (in the step 802).

Thereafter, the file access portion 100 determines the formats of the user ID and the access authority in accordance with the machine ID (in the step 803).

Thereafter, the file access portion 100 determines whether or not the formats being determined are matched with those of the local computer system (in the step 804).

When the file access portion 100 determined that the formats were not matched, it converts the formats of the user ID and the access authority stored in the conversion rule storage portion 33, 43 into those of the local computer system 30, 40 (in the step 805).

Thereafter, the file access portion 100 determines whether or not to accept the file access in the procedure shown in Fig. 7 in accordance with the user ID and the access authority where their formats have been converted (in the step 806).

Thus, according to the computer network of the present invention, even if the formats of the user ID and the access authority of one computer system 20, 30, 40 differ from those of the other computer system 20, 30, 40, by compensating the differences with the conversion rules, a remote file access can be validly performed without necessity of a special procedure.

Claims

(1) A computer network connected with a plurality of computer systems through a communication medium for accessing files that said plurality of computer systems have from all of said plurality of computer systems, each of said plurality of computer systems comprising:

access authority information storage means for storing information with respect to access authority in accordance with an owner ID;

means for determining whether or not a format of said user ID and said access authority being received accord with a format of own user ID and own access authority when a remote access is accepted;

means for converting the format of said user ID and said access authority being received into the format of own user ID and own access authority in accordance with a predetermined conversion rule when the format of own user ID and access authority is not matched with the format of said user ID and said access authority being received.

means for comparing said user ID and said access authority whose format has been converted with information of said access authority stored in said access authority storage means and for determining whether or not to execute said remote access.

(2) A computer network connected with a plurality of computer systems through a communication medium for accessing files that said plurality of computer systems have from all of said plurality of computer systems, each of said plurality of computer systems comprising:

access authority information storage means for storing information with respect to access authority in accordance with an owner ID;

means for adding a machine ID to a user ID and for sending the resultant ID to another computer system of said plurality of computer systems when a remote accest request is issued;

means for determining whether or not a format of said user ID and said access authority being received accord with a format of own user ID and own access authority when a remote access is accepted;

conversion rule storage means for storing a rule for converting a format of said user ID and said access authority;

means for converting the format of said user ID and said access authority being received into the format of own user ID and access authority in accordance with a conversion rule stored in said conversion rule storage means when the format of own user ID and access authority is not matched with the format of said user ID and said access authority being received; and

means for comparing said user ID and said access authority whose format hat been converted with information of said access authority stored in said access authority storage means and for determining whether or not to execute said remote access.

(3) The computer network as set forth in claim 1, wherein each of said plurality of computer systems further comprises means for determining whether or not a file with respect to an access request is present in own computer system and for requesting a remote access when the file is not present.

(4) The computer network as set forth in claim 2, wherein each of said plurality of computer systems further comprises means for determining whether or not a file with respect to an access request is present in own computer system and for requesting a remote

access when the file is not present.

(5) A file access method of remotely accessing a file among a plurality of computer systems connected through a communication medium, said method comprising the steps of:

adding a machine ID to a user ID and for sending the resultant ID to another computer system of said plurality of computer systems when a remote access request is issued in said plurality of computer systems;

determining whether or not a format of said user ID and said access authority being received accord with a format of own user ID and own access authority when a remote access is accepted in said plurality of computer systems;

converting the format of said user ID and said access authority being received into the format of own user ID and own access authority in accordance with a predetermined conversion rule when the format of own user ID and access authority is not matched with the format of said user ID and said authority being received; and

comparing said user ID and said access authority whose format has been converted with information of said access authority stored in said access authority storage means and for determining whether or not to execute said remote access.

(6) The file access method as set forth in claim 5, wherein said method further comprises the step of determining whether or not a file of which an access request is issued in one of said plurality of computer systems is present in own computer system and for issuing a remote access request when the file is not present in own computer system.

FIG. 1

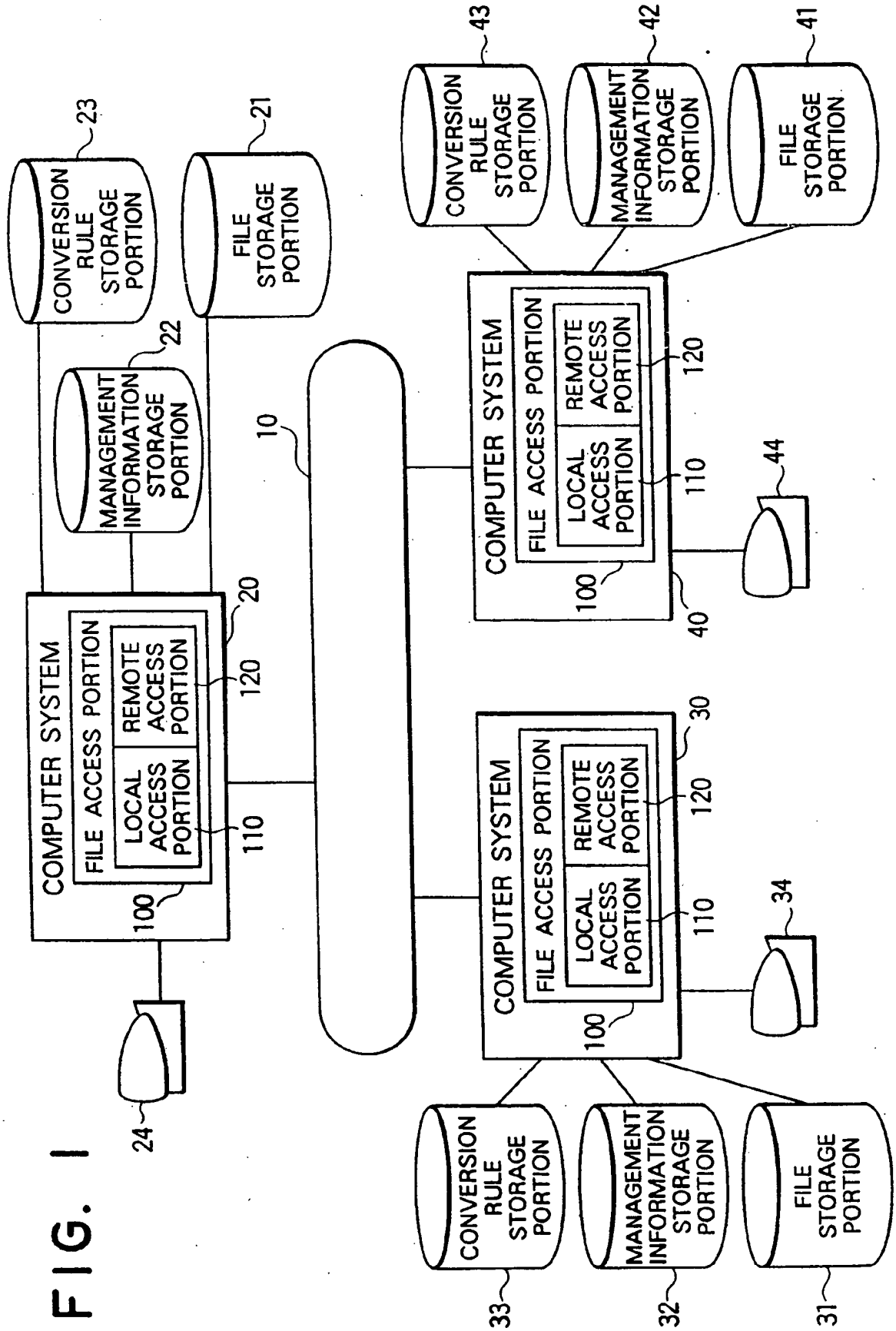

CONVERSION RULE STORAGE PORTION
23
FILE STORAGE PORTION
21
MANAGEMENT INFORMATION STORAGE PORTION
22
10
COMPUTER SYSTEM
FILE ACCESS PORTION
LOCAL ACCESS PORTION
REMOTE ACCESS PORTION
20
120
110
100
24
CONVERSION RULE STORAGE PORTION
43
MANAGEMENT INFORMATION STORAGE PORTION
42
FILE STORAGE PORTION
41
COMPUTER SYSTEM
FILE ACCESS PORTION
LOCAL ACCESS PORTION
REMOTE ACCESS PORTION
120
110
100
40
44
COMPUTER SYSTEM
FILE ACCESS PORTION
LOCAL ACCESS PORTION
REMOTE ACCESS PORTION
30
120
110
100
34
CONVERSION RULE STORAGE PORTION
33
MANAGEMENT INFORMATION STORAGE PORTION
32
FILE STORAGE PORTION
31

FIG. 2

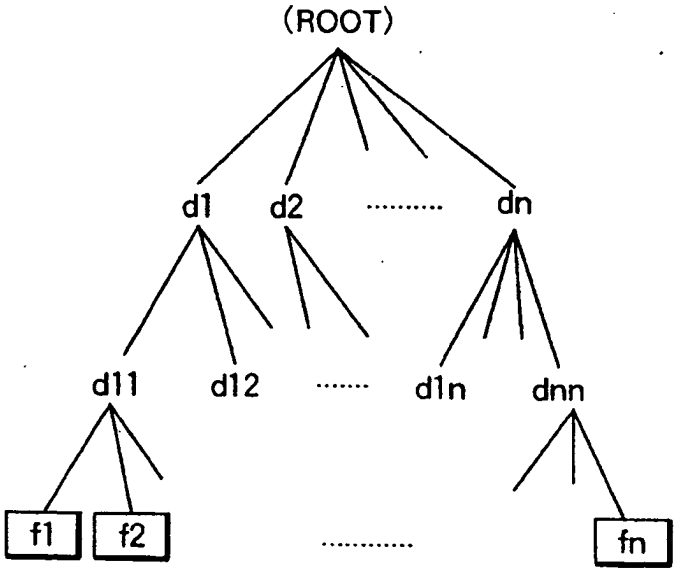

(ROOT)
d1
d2
dn
d11
d12
d1n
dnn
f1
f2
fn

FIG. 3

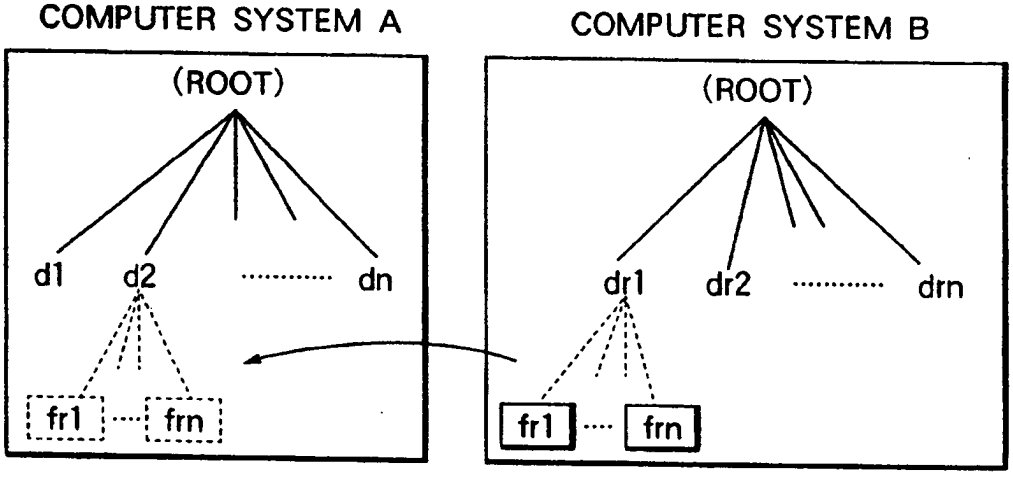

COMPUTER SYSTEM A
(ROOT)
d1
d2
dn
fr1
frn
COMPUTER SYSTEM B
(ROOT)
dr1
dr2
drn
fr1
frn

FIG. 4

ACCESS AUTHORITY / ID	READ	WRITE	EXECUTE	MOVE	DELETE
OWNER PERSONAL	○	○	○	○	○
OWNER GROUP	–	○	–	○	○
OTHER	–	○	–	–	–

○ REPRESENTS PRESENCE OF AUTHORITY.

FIG. 5

A / B	READ	WRITE	EXECUTE	MOVE	DELETE
READ	○	–	–	–	–
WRITE	–	○	–	○	○
EXECUTE	–	–	○	–	–

FIG. 6

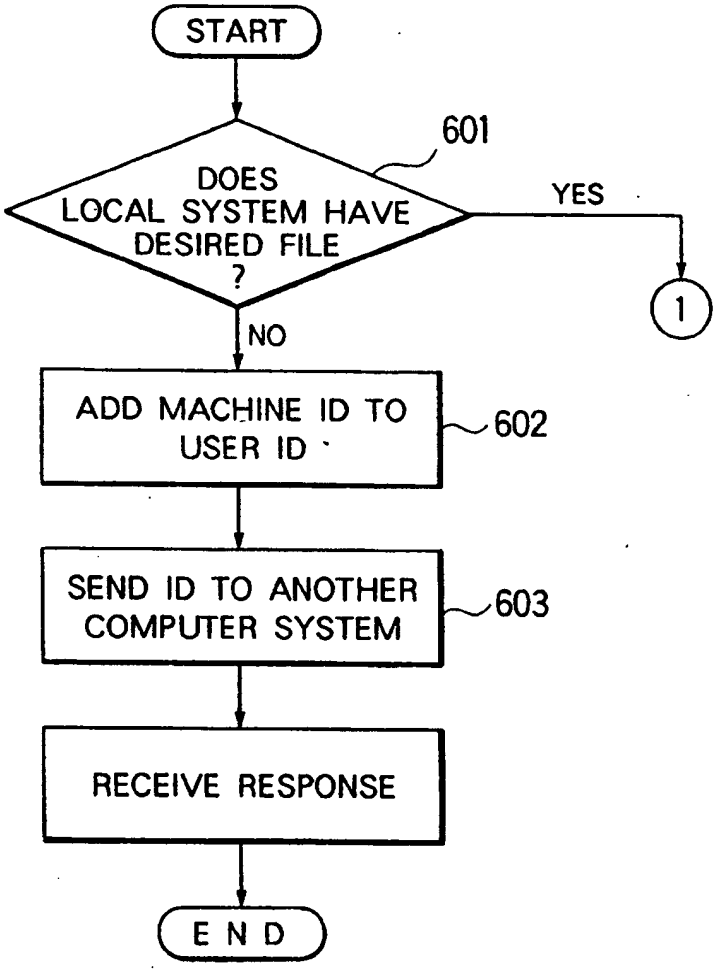

START
601
DOES LOCAL SYSTEM HAVE DESIRED FILE ?
YES
1
NO
ADD MACHINE ID TO USER ID
602
SEND ID TO ANOTHER COMPUTER SYSTEM
603
RECEIVE RESPONSE
END

FIG. 7

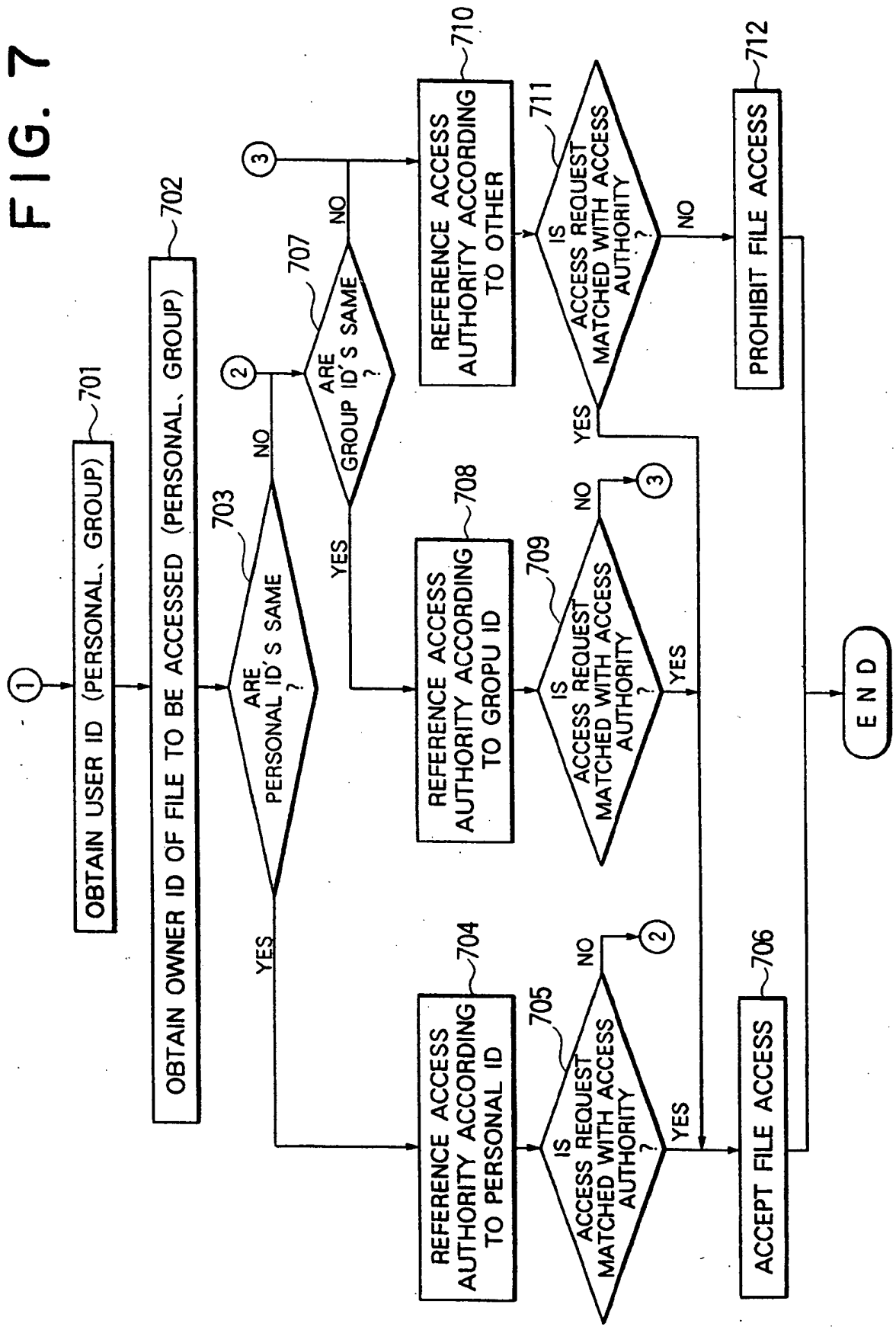
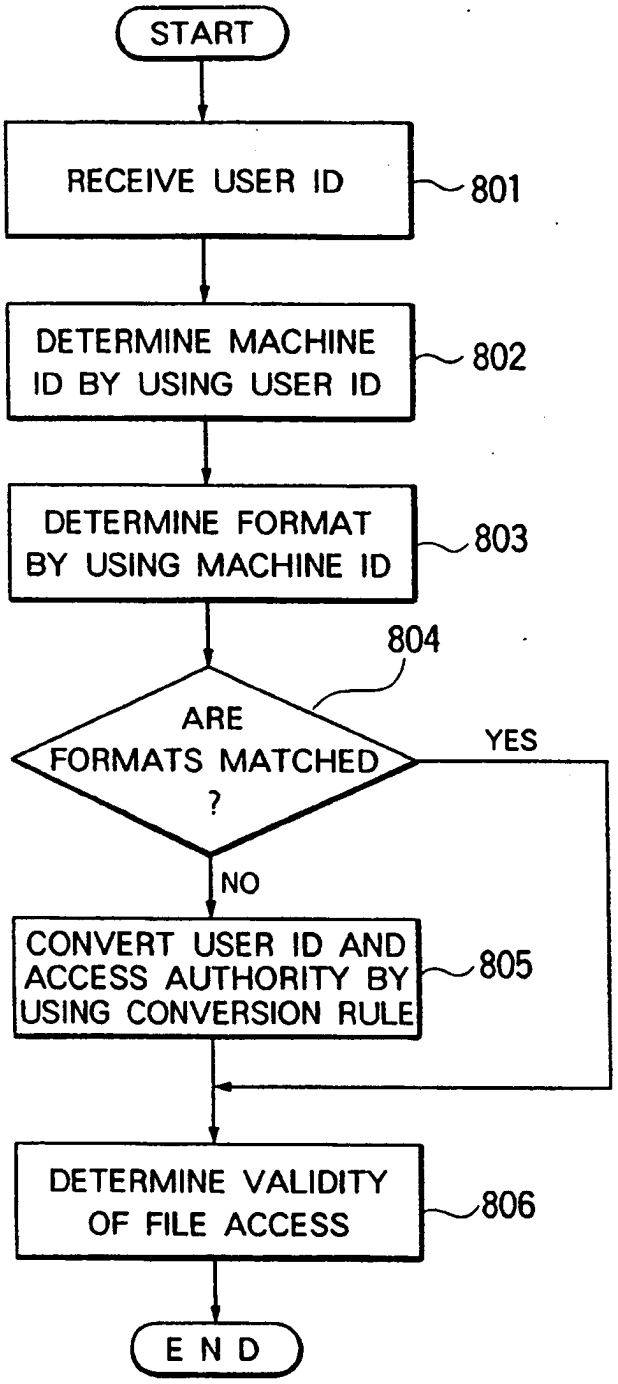

①
OBTAIN USER ID (PERSONAL、GROUP)
701
OBTAIN OWNER ID OF FILE TO BE ACCESSED (PERSONAL、GROUP)
702
ARE PERSONAL ID'S SAME ?
703
YES
NO
②
ARE GROUP ID'S SAME ?
707
YES
NO
③
REFERENCE ACCESS AUTHORITY ACCORDING TO PERSONAL ID
704
REFERENCE ACCESS AUTHORITY ACCORDING TO GROPU ID
708
REFERENCE ACCESS AUTHORITY ACCORDING TO OTHER
710
IS ACCESS REQUEST MATCHED WITH ACCESS AUTHORITY ?
705
709
711
YES
NO
ACCEPT FILE ACCESS
706
PROHIBIT FILE ACCESS
712
END

FIG. 8


START
RECEIVE USER ID
801
DETERMINE MACHINE ID BY USING USER ID
802
DETERMINE FORMAT BY USING MACHINE ID
803
804
ARE FORMATS MATCHED ?
YES
NO
CONVERT USER ID AND ACCESS AUTHORITY BY USING CONVERSION RULE
805
DETERMINE VALIDITY OF FILE ACCESS
806
E N D

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number : **0 477 039 A3**

(12) EUROPEAN PATENT APPLICATION

(21) Application number : **91308667.4**

(51) Int. Cl.[5] : **G06F 9/445**, G06F 1/00

(22) Date of filing : **20.09.91**

(30) Priority : **21.09.90 JP 252864/90**

(43) Date of publication of application :
25.03.92 Bulletin 92/13

(84) Designated Contracting States :
DE FR GB

(88) Date of deferred publication of search report :
16.12.92 Bulletin 92/51

(71) Applicant : **KABUSHIKI KAISHA TOSHIBA**
72, Horikawa-Cho Saiwai-ku
Kawasaki-shi Kanagawa-ken (JP)

(72) Inventor : [redacted] **c/o Intellectual Property Division**
Kabushiki Kaisha Toshiba, 1-1, Shibaura 1-chome
Minato-ku, Tokyo (JP)

(74) Representative : **Luckhurst, Anthony Henry William et al**
MARKS & CLERK 57-60 Lincoln's Inn Fields
London WC2A 3LS (GB)

(54) Computer network.

(57) Each computer system of the computer network according to the present invention has a management information storage portion for storing information with respect to an access authority in accordance with an owner ID and a conversion rule storage portion for storing a rule for converting the formats of a user ID and an access authority. Each computer system adds a machine ID to a user ID and sends the resultant ID to another computer system when a remote access request is issued. In addition, the computer system determines whether or not the formats of the user ID and the access authority being received accord with those of a local computer system when a remote access is accepted. The computer system converts the formats of the user ID and the access authority being received into those of the local computer system in accordance with a predetermined conversion rule when the formats of the local computer system are not matched with those on the remote computer system. Thereafter, the computer system compares the user ID and the access authority whose formats have been converted with information of the access authority stored in the access authority storage portion and determines whether or not to execute the remote access.

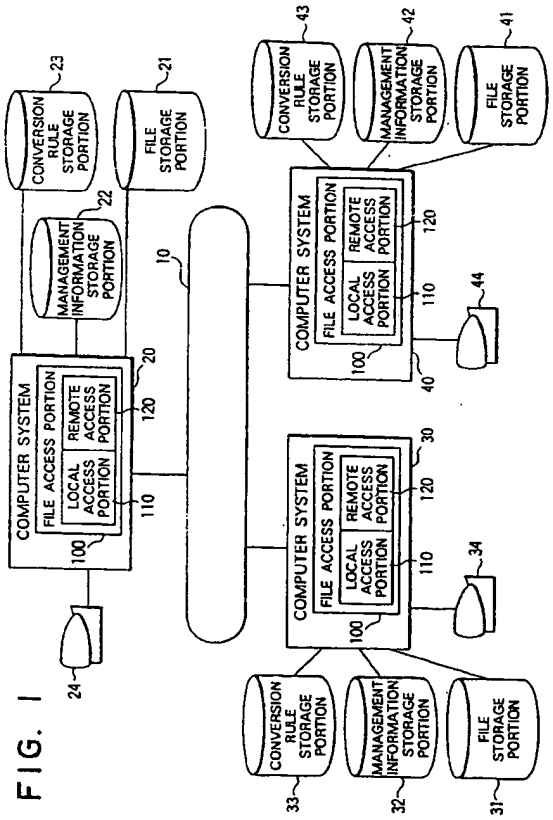


FIG. 1

EP 0 477 039 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 91 30 8667
Page 1

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl.5)
Y	PROCEEDINGS OF THE SIXTH SYMPOSIUM ON RELIABILITY IN DISTRIBUTED SOFTWARE AND DATABASE SYSTEMS 17 March 1987, WILLIAMSBURG, VA, USA pages 84 - 92 C.Y. WANG ET AL. 'Access Control in a Heterogeneous Distributed Database Management System' * page 84, left column, line 35 - page 85, right column, line 31 * * figure 1 * ---	1-6	G06F9/445 G06F1/00
Y	COMPUTERS & SECURITY. INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY vol. 5, no. 4, December 1986, AMSTERDAM NL pages 314 - 324 P.A.KARGER 'Authentication and Discretionary Access Control in Computer Networks' * page 315, left column, line 10 - line 12 * * page 315, left column, line 29 - line 35 * * page 321, left column, line 11 - line 32 * * page 321, right column, line 33 - page 322, left column, line 3 * --- -/--	1-6	TECHNICAL FIELDS SEARCHED (Int. Cl.5) G06F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	02 OCTOBER 1992	SCHARFENBERGER B.

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P0401)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number

EP 91 30 8667

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl.5)
Y	PROCEEDINGS OF THE 1986 IEEE SYMPOSIUM ON SECURITY AND PRIVACY 7 April 1986, OAKLAND, CA, USA pages 204 - 222 D.M.NESSETT 'Factors Affecting Distributed System Security' * page 217, left column, line 34 - line 47 * * page 217, right column, line 20 - line 24 * * page 217, right column, line 34 - line 40 *	1-6	
Y	SYSTEMS INTERNATIONAL vol. 14, no. 7, July 1986, GB pages 51 - 54 A.OSADZINSKI 'Remote File Access' * page 51, right column, line 14 - line 19 * * page 51, right column, line 46 - line 49 *	3-4,6	
A	UNISPHERE vol. 8, no. 6, September 1988, US pages 64 - 68 R.REINAUER 'UNIX System V.3 Remote File Sharing' * the whole document *	1-6	TECHNICAL FIELDS SEARCHED (Int. Cl.5)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	02 OCTOBER 1992	SCHARFENBERGER B.

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P0401)